IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

CROWDSTRIKE, INC.,	)	
	)	
Plaintiff,	)	
	)	C.A. No. 17-146-GMS
v.	)	
	)	**REDACTED PUBLIC**
NSS LABS, INC.,	)	**VERSION**
	)	
Defendant.	)	Demand for Jury Trial

SECOND AMENDED COMPLAINT

Plaintiff CrowdStrike, Inc. ("CrowdStrike" or "Plaintiff"), by and through counsel, respectfully submits its Second Amended Complaint against the Defendant as follows:

I. PRELIMINARY STATEMENT

1. Defendant NSS Labs, Inc. ("NSS" or "Defendant") has unlawfully accessed, copied, used and misappropriated CrowdStrike's Falcon Platform in violation of federal law.

2. CrowdStrike's Falcon Platform ("Falcon Platform") is a proprietary software-as-a-service cybersecurity product. It consists of software, databases, computer systems, and user interfaces hosted by CrowdStrike in the cloud ("Falcon Cloud"), and a lightweight software agent that authorized users can download onto their endpoint devices ("Falcon Agent"). The Falcon Cloud and Falcon Agent (together the "Falcon Platform") work in communication with each other to provide comprehensive cybersecurity protection and feedback to enterprise clients. The Falcon Platform is password protected, and users must obtain CrowdStrike's authorization before accessing and using it.

3. NSS is a for-profit business in the cybersecurity market. It generates revenue by testing cybersecurity products and monetizing the results. In addition to selling testing reports and

marketing rights, including to the vendors mentioned in the reports, it uses information gleaned from testing vendor products to build and market its own cybersecurity product, the Cyber Advanced Warning System ("CAWS").

4. NSS has a long history of questionable business practices, including misrepresenting the validity and independence of its tests and reports. According to other security vendors, NSS misrepresents the scope of its testing practices, unfairly tests obsolete products against up-to-date ones without disclosing it, conceals which vendors tuned their products before testing and which did not, pressures vendors to pay for private testing in advance of "public" comparative testing and exhibits bias in favor of vendors who pay for testing (*i.e.* "pay-to-play").

5. In 2016, CrowdStrike learned that NSS planned to conduct a competitive test of certain cybersecurity products, sometimes referred to as advanced endpoint protection ("AEP") products. CrowdStrike was interested in participating in such a test, but was hesitant because NSS had a poor reputation and had never tested AEP products before. NSS told CrowdStrike that CrowdStrike [redacted].

6. Under the circumstances, CrowdStrike decided to pay NSS to conduct two private tests because NSS had never done this type of testing before; it wanted to show NSS how to properly set up and test the CrowdStrike product; and NSS represented that [redacted]. As part of the private tests, CrowdStrike gave NSS access to the Falcon Platform pursuant to a written contract for the limited purpose of conducting those two tests. The agreement expressly prohibited NSS from using or disclosing the results of those tests. Unfortunately, the NSS private tests failed to adhere to NSS' stated methodology and exhibited critical flaws and quality control problems. NSS' CEO, Vikram Phatak, and NSS' Vice

President of Operations, Lisa Owen, admitted that the private testing and results were flawed and offered to perform a third test for free.

7. NSS then told CrowdStrike that the third test would have to wait because NSS was too busy performing its comparative AEP test. Because NSS failed to address the admitted flaws in its private testing of the Falcon Platform, among other reasons, CrowdStrike had no confidence that NSS had the ability to perform a meaningful test and declined to authorize NSS to access and use the Falcon Platform for the AEP competitive testing. CrowdStrike told NSS specifically on multiple occasions that NSS was not authorized to access or use CrowdStrike's Falcon Platform for that purpose. CrowdStrike also sent NSS a copy of its standard Terms and Conditions of service, highlighting that competitive analysis was prohibited and that no CrowdStrike customer could authorize NSS to access the Falcon Platform for such testing.

8. Undeterred, NSS conspired to illicitly and fraudulently obtain, and then use, confidential CrowdStrike login credentials to access the Falcon Platform. NSS used those stolen credentials eleven times over a week to illegally and fraudulently access, copy and use the Falcon Agent software, intrude into and alter data in a customer's instance of the Falcon Cloud, and manipulate the Falcon Platform to generate data about how it operates, so that NSS could market and sell its testing, testing reports and associated marketing rights, and, on information and belief, use the data to develop, market, and sell CAWS. By its unauthorized actions, NSS violated the Computer Fraud and Abuse Act, infringed CrowdStrike's copyrights, and misappropriated CrowdStrike's trade secrets.

9. CrowdStrike caught NSS' unlawful intrusion in the middle of the competitive testing of the CrowdStrike Falcon Platform, and disabled NSS' use of it. NSS nonetheless proceeded to advertise and publish the test results, even though it knew that the testing (a) was

incomplete, (b) would have produced different results if completed, (c) was not independent or unbiased, (d) did not follow NSS' stated testing methodology, and (e) was flawed like the private tests of the Falcon Platform. The statements NSS published about the Falcon Platform, NSS' methodology, and NSS's independence and lack of bias, were false and misleading, and were made willfully and maliciously by NSS to promote its reports and CAWS product for its own financial gain, in violation of the Lanham Act.

10. CrowdStrike filed its original complaint in this action on February 10, 2017. Since then, NSS has announced that it intends to perform further competitive AEP group testing in late 2017, for publication in 2018. NSS recently attempted to obtain access to the Falcon Platform, including indirectly through a reseller. And, although NSS has stated that CrowdStrike products will not appear in that upcoming AEP group test, when confronted with these attempts to access, NSS still maintains it "has the legal right to publish public tests of all products in the market" and has refused to give assurances that it will not access or use the Falcon Platform. NSS' continuing threats to access and use the Falcon Platform without CrowdStrike's authorization, and publication of false and misleading reports about CrowdStrike, if not enjoined, will continue to cause immediate and irreparable harm to CrowdStrike's business.

II. PARTIES

11. CrowdStrike is a corporation formed under the laws of the State of Delaware with its principal place of business located in Sunnyvale, California.

12. Upon information and belief, Defendant NSS was and is a corporation organized and existing under the laws of the State of Delaware, with its principal place of business in Austin, Texas.

III. JURISDICTION AND VENUE

13. This Court possesses subject matter jurisdiction over CrowdStrike's claims under

28 U.S.C. § 1331 and 28 U.S.C. § 1367.

14. Venue is proper in the United States District Court for Delaware under 28 U.S.C. § 87 and 28 U.S.C. § 1391(b)(1) because the Defendant is incorporated in Delaware, and the contract between the parties stipulates that each party shall submit to the exclusive and personal jurisdiction of the federal courts located in New Castle County, Delaware.

IV. FACTUAL ALLEGATIONS

A. Plaintiff CrowdStrike

15. CrowdStrike is a privately-owned cybersecurity company founded in 2011. The Falcon Platform is its flagship product, resulting from [redacted] in development and years of work by a staff of highly talented engineers. The Falcon Platform is deployed by high-profile enterprises around the world, including financial institutions, health care providers, and energy companies, and has successfully stopped high-profile attacks that other products could not. CrowdStrike's success, in large part due to its Falcon Platform, has made it a prominent figure in the cybersecurity industry.

16. CrowdStrike controls all access to its Falcon Platform through confidential login credentials and licensing agreements. To use the Falcon Platform, licensed users must log into the Falcon Platform and obtain a copy of the Falcon Agent for each "endpoint device" (*e.g.*, computer, laptop, etc.). To begin, a system administrator for the licensed customer receives a Falcon Platform link (usually in an email from CrowdStrike) to activate the account. The system administrator sets a password and dual-factor authentication, and must review and accept the Falcon Platform click-through agreement, before downloading and copying the Falcon Agent to endpoint devices. The system administrator can authorize and add other users [redacted], who can then obtain Falcon Agent software for installation on the customer's systems pursuant to the license. After installation, the Falcon Agent communicates with the customer's instance of the

Falcon Cloud to complete the set-up process.

17. After installation, the Falcon Agent's detection logic monitors and analyzes activity on the endpoint device, and sends certain data to the customer's instance of the Falcon Cloud. When warranted, such as when a threat is detected, applications in the Falcon Cloud direct the Falcon Agent to increase or alter its data collection and provide more information to the customer's instance of the Falcon Cloud for analysis. Collected data is combined with proprietary threat information in CrowdStrike's "ThreatGraph" database in the Falcon Cloud, which uses behavioral pattern matching techniques, machine learning, artificial intelligence, detection logic, user input, and other information to detect patterns indicating possible attacks.

18. A customer's system administrator logs into a web-based user interface ("Falcon Dashboard") using confidential login credentials to view its Falcon Platform data, statistics and analysis. On the Falcon Dashboard, the administrator will find confidential information on what threats were detected, [redacted]. Through the Falcon Dashboard, the system administrator can configure Falcon Platform settings and affect how the system reacts to malware and other threats. For example, an administrator can enable the prevention system and choose between different machine learning methods for identifying potential malware. An administrator can also set different thresholds for malware detection and prevention, such as Disabled, Cautious, Moderate, or Aggressive. A customer may also take raw data from the Falcon Platform and access it elsewhere (e.g., through a third-party threat intelligence platform) by leveraging application programming interfaces ("APIs") to transfer the data. The information a customer receives through an API from the Falcon Platform depends on the customer settings.

19. The Falcon Platform may also include optional functionality and services. For

example, it may include Falcon Spotlight, which provides continuous, real-time assessment of the vulnerability of a system's endpoints; the Falcon Discover solution, which provides a real-time inventory and assessment of applications in the system, enabling administrators to identify vulnerable software for remediation; and, Falcon OverWatch, a proactive search, investigation and advising service provided by CrowdStrike's team of elite security professionals.

20. The Falcon Agent is copyrighted software, registered in the United States Copyright Office as No. TX 8-447-667. The copyright is owned by CrowdStrike.

21. The Falcon Agent and components of the Falcon Cloud constitute and incorporate trade secrets developed by CrowdStrike. CrowdStrike's trade secrets include: [redacted]. These are all matters not generally known, subject to CrowdStrike measures to keep them confidential, and that give CrowdStrike an economic advantage over competitors. For example, a competitor with specific knowledge how [redacted] could use that information to build, advertise and sell its own product.

B. Defendant NSS Labs

22. NSS is a for-profit business that monetizes comparative (published) and private testing services and sells its own cybersecurity product. NSS tests and ranks competitors' cybersecurity products in order to sell reports, subscriptions and marketing rights related to those rankings. It uses this publicity to sell contracts for private testing to vendors that may be the subject of comparative testing. NSS also uses data it collects during testing to populate, develop, market and sell its own competitive CAWS cybersecurity product.

23. NSS generally announces a group test many months before it is set to start. For

example, NSS announced its first AEP test in February 2016 indicating the test would begin many months later, and run for months. NSS announced a second round of AEP testing in April 2017, stating it will begin in the second half of 2017 and the results will be announced in 2018. In the time between announcement and completion of the comparative test, NSS markets and sells confidential "private" tests to vendors who it wants to participate in the group comparative test. On information and belief, NSS sells such private tests for [redacted], and favors paying vendors in its comparative tests.

24. When NSS completes a group test, it publishes a very high-level product comparison score for free download without any detail underlying the score, to advertise its more detailed reports that NSS sells for thousands of dollars. Specifically, it sells detailed individual reports about a single vendor's results, as well as enterprise subscriptions that provide access to a fuller range of vendor data and comparative reports. The high costs of the paid reports mean that many corporations do not buy the paid reports and simply rely on the free high-level product comparison score when assessing which products to purchase.

25. NSS also sells marketing rights to the tested vendors who score well. According to NSS, it will sell vendors the rights to share an NSS Labs report with their customers and prospects for a period of twelve months in various configurations. In 2014, a vendor reported that NSS asks vendors to pay fees that can exceed $100,000 for such marketing rights. Based on this business model, it is necessary for NSS to make sure numerous vendors participate in the group test and that some score well and others perform poorly.

26. Numerous vendors have complained that NSS misrepresents the validity and independence of its reporting business. For example, in 2010, Google claimed that an NSS report rating Microsoft's Edge browser as superior to Google's Chrome browser was biased because

Microsoft was a paid sponsor of the test, the test used an outdated version of Chrome and NSS would not make the testing methodology sufficiently public so that it could be independently verified.[1] When NSS released a similar report in 2017 favoring Microsoft, the results were not surprising to anyone who has followed NSS's tests over the years because it regularly awarded Microsoft browsers the top spots in its malware-blocking evaluations.[2] In 2014, cybersecurity companies FireEye and Palo Alto Networks criticized NSS' business practices on the basis that NSS's sale of marketing rights to the reports incentivized NSS to lower the testing bar to increase the number of vendors who would buy those rights, and that NSS's testing was biased because it employed out-of-date and improperly configured versions of leading products whose vendors declined to participate.[3] NSS is widely known as a pay-to-play testing company, meaning its testing results are biased against companies that do not pay it for testing.

27. NSS also uses the information it learns from testing vendor products to populate, develop, market, and sell its own CAWS Threat Protection Platform. According to NSS' Chief Marketing Officer, Gautam Aggarwal, NSS used information from its point-in-time validation testing (e.g. "private" or comparative tests) to build CAWS 3.0. An NSS patent application on its "Threat and Defense Evasion Modeling System and Method" elaborates that the system is "based on prior testing results" stored in a database. *See* U.S. Patent App. 2015/0310217 ¶ 28. NSS describes building that system from "empirical testing of the products," by creating "databases containing empirical test result data on exploits that bypass security products." *Id.*, ¶¶ 40, 47. A

[1] *See* https://www.pcmag.com/article2/0,2817,2374344,00.asp.
[2] *See* https://www.computerworld.com/article/3233287/web-browsers/microsofts-anti-malware-sniffing-service-powers-edge-to-top-spot-in-browser-blocking-tests.html.
[3] *See* http://www.crn.com/print/news/security/300072250/palo-alto-networks-fireeye-criticize-nss-labs-testing-firm-defends-itself.htm; https://researchcenter.paloaltonetworks.com/2014/09/response-recently-released-2014-nss-next-generation-firewall-comparative-analysis/.

CAWS user then inputs a selection of security products it uses, and receives information on "the efficacy" of that selection, including what vulnerabilities may have "the ability to bypass each security product selected." *Id.*, ¶¶ 28,44. On information and belief, the NSS patent application describes how NSS uses information from vendor testing to build the CAWS system.

28. On information and belief, NSS sells access to the CAWS Platform, specifically release 3.0, that uses information from NSS' testing of CrowdStrike's Falcon Platform. NSS advertises an individual license to use CAWS in the Advanced Endpoint Protection (AEP) category for $3,490 per year. NSS advertises that it sells access to all the CAWS security categories for over ten thousand dollars.

C. CrowdStrike's Contractual Relationship with NSS

29. In early 2016, CrowdStrike provided NSS labs with limited access to its Falcon Platform for the sole purpose of performing private, confidential testing. The parties entered into a number of agreements that expressly reserved CrowdStrike's ownership and control of its confidential information and stated that comparative testing of the Falcon Platform was unauthorized.

30. On or about January 5, 2016, CrowdStrike and NSS executed a Mutual Non-Disclosure Agreement attached as **Exhibit 1** (the "NDA"). The NDA [redacted]. NDA ¶ 1. It also limited NSS to [redacted]. NDA ¶¶ 2,6,10. Through the NDA, NSS agreed [redacted] NDA ¶ 3.

31. Similar provisions were incorporated into the private testing agreement for the Falcon Platform executed by CrowdStrike and NSS around April 11, 2016, attached as **Exhibit 2** (the "Private Agreement").

32. Under the Private Agreement, CrowdStrike retained [redacted]. The Private Agreement incorporates confidentiality terms from NSS' online terms of service ("TOS"). Private Agreement at 1. The TOS, attached as **Exhibit 3**, provides that neither party [redacted] TOS ¶ 2. "Confidential Information" is defined broadly in these provisions, as [redacted] TOS ¶ 2. Confidential information specifically includes, but is not limited to, [redacted] *Id.* Separately, the Private Agreement reaffirms that the results of the test to be provided by NSS to CrowdStrike pursuant to the engagement [redacted] Private Agreement, 1(e).

33. The Private Agreement also makes clear that CrowdStrike's [redacted]. *Id.*, Ex. A ¶ 1.

34. As the Private Agreement shows, CrowdStrike's [redacted]. For example, CrowdStrike was required to provide [redacted]. *Id.* ¶ 3(d). This required CrowdStrike to disclose [redacted]. According to the Private Agreement, the [redacted]

[redacted]. *Id.*, ¶¶ 3, 3(d).

35. NSS also promised [redacted]. *Id.*, Ex. A, ¶¶ 3, 5. NSS also agreed it would not, under any circumstances, [redacted] *Id.*

36. The Private Agreement provides remedies in [redacted] Private Agreement 6(b).

37. The Private Agreement specifically provides for remedies of [redacted] *Id.* ¶ 6(b)-(d).

D. NSS's Private Testing of CrowdStrike's Falcon Platform

38. Around mid-2016, NSS provided private testing results on the Falcon Platform's advanced endpoint detection features to CrowdStrike. NSS' report demonstrated severe flaws and quality control issues and NSS' failure to adhere to its stated methodologies. For example, NSS had incorrectly identified a large percentage of samples as malicious. NSS' results also did not match what the Falcon Platform actually reported. For example, NSS' report stated that the Falcon Platform failed to detect some malware in cases where the Falcon Platform logs recorded a detection. On information and belief, these errors were caused by NSS [redacted]

[redacted].

When CrowdStrike pointed out the problems, NSS promised to fix the issues in a second private test.

39. Later in 2016, NSS conducted additional private testing and provided a second report to CrowdStrike. NSS' second round of private testing exhibited similar flaws and quality control defects as the first test. For example, almost 25% of the "malware" NSS used in the testing was not actually malicious, including prominent and widely-used programs like Microsoft's Skype and Mozilla's Firefox that no reputable testing firm would claim to be malware. NSS conceded that that the Falcon Platform received a low performance score because it had failed to identify programs such as Skype and Firefox as malware, even though those programs were not malware. Furthermore, NSS' results again did not match those reported by the Falcon Platform.

40. On January 18, 2017, Dmitri Alperovitch, Chief Technology Officer and co-founder of CrowdStrike, discussed these results with Vikram Phatak and Jason Brvenik of NSS. Mr. Phatak admitted that the second round of NSS testing on the Falcon Platform had not complied with NSS' own testing standards. Mr. Phatak conceded that NSS' inappropriate labelling of widely-used programs such as Skype and Firefox as "malware" made the tests flawed and skewed the results. Alperovitch Decl. ¶ 23, attached as **Exhibit 7.**

41. To address NSS' repeated testing failures, Mr. Phatak offered CrowdStrike a third round of testing without charge. However, NSS refused to perform that third test at the time because, as it explained, it was focusing its efforts on a scheduled group comparative test of all AEP vendors including CrowdStrike. *Id.* ¶ 24.

E. CrowdStrike Refuses to Participate in "Public" Testing

42. As it had indicated previously, CrowdStrike would not and did not authorize access

to the Falcon Platform for comparative testing given the fundamental flaws with NSS' testing methodologies.

43. Nonetheless, Mr. Phatak stated that NSS had obtained credentials to access the Falcon Platform through a third party, and intended to use them to perform a comparative test and sell the report publicly, irrespective of CrowdStrike's authorization. *Id.*

44. In response, Mr. Alperovitch informed NSS that CrowdStrike did not consent, and had expressly declined, to participate in any comparative testing of CrowdStrike products. He also expressly told NSS that use of the Falcon Platform for comparative testing through a CrowdStrike customer violated Crowdstrike's standard customer Terms and Conditions of service (and the Private Agreement), and that NSS was otherwise unauthorized by CrowdStrike. *Id.* ¶ 25.

45. As such, no later than January 18, 2017, NSS and its CEO, Mr. Phatak, were aware that (1) CrowdStrike's Terms and Conditions did not permit comparative testing; (2) that NSS' testing would breach CrowdStrike's Terms and Conditions; (3) that any access by NSS of CrowdStrike's Falcon Platform was unauthorized; and (4) that the copying and use of any CrowdStrike software by NSS was unauthorized.

46. On January 19, 2017, Mr. Alperovitch sent Mr. Phatak an email reiterating these points, reconfirming that "to the extent a customer of ours provided you with our software it would be a direct violation of our Terms of Service," and providing an electronic link to CrowdStrike's Terms and Conditions of service. *Id.*, Ex. 8. Mr. Alperovitch also excerpted in full the "Restrictions" portion of the Terms and Conditions, which state that a person "may not access or use the Products: (i) if you are a CrowdStrike Competitor or on behalf of a CrowdStrike Competitor, or (ii) to perform any competitive analysis on the Products." *Id.* The Terms and Conditions prohibit a user to "sublicense, distribute or otherwise transfer the Products to any third party" or

"allow third parties to access or use the Products" except for certain expressly permitted "Internal Use." The Terms and Conditions expressly prohibit any "attempt to gain unauthorized access to the Products or their related systems or networks." *Id.*, Ex. 6 ¶ 3.1, 3.2.

47. In disregard of these limitations on a CrowdStrike customer's use of CrowdStrike's intellectual property, on January 19, 2017, Mr. Phatak responded that NSS took "a different view" of the situation, and would not be deterred from its comparative test plans. *Id.*, Ex. 8.

48. On January 27, 2017, CrowdStrike's attorney sent a letter to NSS, demanding that NSS not use CrowdStrike Falcon Platform in a comparative test, and demanding the return or destruction of all copies of CrowdStrike's Falcon Platform software, and any unauthorized testing data. **Exhibit 8**. He reiterated that any access or use by NSS of CrowdStrike software obtained from a CrowdStrike customer would be unauthorized, breach NSS' agreement with CrowdStrike, and breach the customer's Terms and Conditions of service with CrowdStrike. *Id.*

49. NSS refused to return CrowdStrike's Falcon Platform and other Confidential Information in direct violation of the NDA, Private Agreement and the customer's Terms and Conditions of service, and proceeded with its plans to intrude into CrowdStrike's Falcon Platform without authorization.

F. NSS' Conspiracy to Fraudulently and Unlawfully Access, Copy and Use the Falcon Platform

50. Because CrowdStrike refused to give NSS access for comparative testing, NSS orchestrated a scheme to covertly and fraudulently obtain CrowdStrike login credentials. NSS engaged third parties to obtain CrowdStrike credentials and provide those to NSS, so it could fraudulently and illegally access CrowdStrike's Falcon Platform.

51. In or before December 2016, on information and belief, NSS engaged David Thomason, of Thomason Technologies LLC ("Thomason"), to find a company willing to contract

with CrowdStrike for a Falcon Platform pilot license under the guise of being a potential customer. On information and belief, David Thomason was the mark because he was a former colleague of NSS CTO Jason Brvenik. Apparently to induce the company to participate in its unlawful scheme, NSS agreed [redacted].

52. On or about January 5, 2016, Thomason submitted a fraudulent purchase order purportedly on behalf of [redacted] for a license to use CrowdStrike's proprietary Falcon Platform, attached as **Exhibit 4.** According to NSS, Thomason knew that the purchase order was for NSS to gain access, but Thomason concealed that from the purchase order to deceive CrowdStrike into making the sale.[4] As part of the fraudulent purchase, [redacted] and Thomason agreed to CrowdStrike's Terms and Conditions, attached as **Exhibit 5.** As described above, those Terms and Conditions limited use of the Falcon Platform to the customer's internal use, and prohibited use of the Falcon Platform (1) by or on behalf of any CrowdStrike competitors, (2) for competitive analysis, or (3) by any third parties except for certain customer "Internal Uses." The CrowdStrike quote/order, signed by Thomason, explicitly stated that [redacted] **Exhibit 4.**

53. According to NSS' Vice President of Operations Lisa Owen, [redacted] and NSS expressly agreed that [redacted], evidencing NSS's conspiracy to defraud CrowdStrike. On information and belief, Thomason also provided CrowdStrike's confidential pricing information to NSS.

54. CrowdStrike was never paid for [redacted] Falcon Platform pilot license.

[4] *See* Transcript of February 10, 2017 Hearing, at 10:12-15; *see also* Dkt. No. 8, ¶ 21. [redacted] claims it did not authorize NSS to access the software. **Exhibit 6.**

55. Around January 25, 2017, CrowdStrike created confidential Falcon Platform credentials for Thomason at [redacted] request. To do this, CrowdStrike [redacted].

56. On information and belief, Thomason provided to NSS the fraudulently obtained login credentials to access [redacted] instance of the Falcon Platform.

57. CrowdStrike's internal computer records demonstrate that someone created an account for a Thomason user on January 25, 2017 and logged in once. The user enabled two-factor authentication pursuant to CrowdStrike's security protocol.

58. Using that Thomason account, someone then created a second user account under the name "Randy" on January 25, 2017, again enabling two-factor authentication. As described above, pursuant to CrowdStrike's protocols, a new user must log in and enable two-factor authentication and then click-through CrowdStrike agreements before downloading the Falcon Agent. On information and belief, that user must have [redacted].

59. CrowdStrike's internal computer records show 11 logins by the user "Randy" on January 25th, 26th, 28th, 29th and 31st. NSS has never denied that this account was used and that these logins were made by an NSS employee. There was an NSS employee named Randy in its Austin facility.

60. On information and belief, NSS downloaded and copied the Falcon Agent on NSS machines, and logged into and accessed the Falcon Platform without authorization and using the fraudulent credentials, to perform comparative testing during the period of January 25-31, 2017.

61. On information and belief, NSS individuals who had access to CrowdStrike confidential information through the private test agreement were also involved in the comparative tests involving CrowdStrike's Falcon Platform. For example, NSS' [redacted] and he is also listed as an "Author" of the Advanced Endpoint Protection Comparative Report Security Value Map, dated February 14, 2017, including CrowdStrike products.

62. On information and belief, during this period, NSS subjected endpoint device(s) loaded with the Falcon Agent to manufactured and fake attacks. On information and belief, the Falcon Agent collected information from and about these fake attacks and sent it to the Falcon Cloud. On information and belief, the Falcon Cloud requested additional information about the fake attacks from the Falcon Agent, and collected that information.

63. During the period of testing, NSS misappropriated and misused CrowdStrike's trade secrets by obtaining and using CrowdStrike's confidential login credentials, downloading and using CrowdStrike's Falcon Agent software, and accessing and using the Falcon Cloud, including ThreatGraph, Falcon Dashboard, and other elements of the Falcon Platform, all without authorization. In addition, NSS misappropriated and misused CrowdStrike's trade secrets through performance of its testing, which involved accessing, acquiring and using information on how the elements of the Falcon Platform handle certain threats and how they interact with each other to provide comprehensive security. For example, NSS' unauthorized testing enabled it to access information on the capabilities and scope of the Falcon Platform, including how its components respond to certain threats under certain conditions. Similarly, by observing and manipulating the Falcon Dashboard user interface, NSS could collect information on Falcon Platform methods and operation exposed there, including information on [redacted]

[redacted]. Such information on CrowdStrike's methods, operation, and capabilities is competitive information that NSS could use to prepare reports that CrowdStrike customers and competitors would buy, and that the latter could leverage to sell their own products. NSS could also use such competitive information to build and sell its CAWS product.

64. Because of NSS's unauthorized intrusion and introduction of fake attacks into the CrowdStrike Falcon Platform, CrowdStrike was forced to divert computing and personnel resources in response. Additionally, data on the fake attacks NSS initiated was introduced into and altered data in [redacted] instance of the Falcon Platform. A [redacted] system administrator using the Falcon Dashboard during the testing would have seen malware and new computers inexplicably appearing in their environment, and received an incorrect and skewed threat assessment for its environment.

65. Because of NSS's unauthorized intrusion and introduction of fake attacks into the CrowdStrike Falcon Platform, Falcon OverWatch was forced to expend resources over January 28-30, 2017 detecting, investigating and responding to NSS' unauthorized access.

66. On January 31, 2017, after detecting NSS' unauthorized intrusion into the system, CrowdStrike disabled the Thomason account, including the credentials for "Randy." Many segments of NSS' testing were not complete when the account was disabled. Dkt. No. 8, Ex. 1.

67. When CrowdStrike contacted David Thomason as part of its investigation, he was not initially forthcoming about how NSS had obtained access to the system. After a number of attempts, Mr. Thomason finally admitted that NSS had approached him and asked him to arrange for a client to buy a Falcon Platform license so that NSS could covertly use it. CrowdStrike asked Mr. Thomason to tell NSS to cease and desist its use of CrowdStrike's systems.

68. On information and belief, shortly thereafter, Thomason contacted NSS and instructed NSS that the results of any testing done on CrowdStrike's software were not to be published and all data regarding the testing of CrowdStrike must be deleted.

69. On February 8, 2017, [redacted] emailed NSS, first saying that NSS had no authorization, then clarifying that NSS had never had authorization, to use [redacted] copy of CrowdStrike's software. The email instructed NSS to delete any tests or data resulting from the use of [redacted] copy of CrowdStrike's software. **Exhibit 6.**

70. On or around February 14, 2017, NSS published a number of free and paid AEP reports, including technical and pricing data on the CrowdStrike Falcon Platform.

71. Shortly thereafter, NSS contacted CrowdStrike customers, telling them that CrowdStrike's products had issues and were leaving them vulnerable, specifically suggesting to them that they should buy NSS' report to learn more.

72. Shortly after its comparative testing, on or around March 2, 2017, NSS released a beta version of its CAWS 3.0 product, announcing the official product on July 18, 2017. NSS' advertising promoted that the CAWS 3.0 product "leverages [NSS'] unmatched expertise in security product testing," and that it would address customers' needs for "empirical data" on their security tools, enabling them to see how security tools behave under "out-of-the-box," "vendor-recommended," and "enterprise-specific" settings, providing insights into threats that might impact programs and computer systems in an enterprise's environment. Similar capabilities are offered by CrowdStrike, including its Falcon Spotlight, which gives security teams a continuous and real-time assessment of the vulnerability exposure of their endpoints, and Falcon Discover, which provides a real-time inventory and assessment of applications in the system.

73. On information and belief, CAWS 3.0 contains testing data relating to

CrowdStrike's Falcon Platform, and that information was obtained and used without authorization. NSS further misappropriated CrowdStrike trade secrets to the extent it accessed and used them to develop CAWS 3.0, such as how the Falcon Platform handles certain threats, how it operates in certain modes, or under different settings. On information and belief, NSS desired, sought, and obtained access to Falcon Platform raw API data for incorporation into CAWS.

74. Both NSS' private and illicit comparative testing of CrowdStrike's Falcon Platform fell short of the Anti-Malware Testing Standards Organization (AMTSO) Fundamental Principles of Testing, although NSS has previously claimed to follow AMTSO guidelines and best practices.

G. NSS False and Misleading Statements

75. On and after February 14, 2017, NSS published a number false and misleading statements about its AEP testing and CrowdStrike's Falcon Platform, including mispresenting the validity of its ranking of the Falcon Platform and its adherence to its own AEP testing methodology.

76. For example, NSS published on its website a free, high-level summary document called the "AEP Comparative Report Security Value Map" and a "Security Value Map graphic." NSS uses these free summary documents to advertise and sell access to the full, underlying paid reports, as discussed above. However, many customers use the free Value Maps in their competitive sales cycle, and never pay for the full reports. These two published documents are false and misleading in a number of ways.

77. The Security Value Map materials give CrowdStrike's Falcon Platform a very poor rating, but fail to mention that those ratings were based on incomplete and flawed data, and that they would have been different if testing was complete. Specifically, the document gives Falcon Host (the prior name for Falcon Platform) a summary product guidance rating of "Caution," but nowhere mentions the known and admitted flaws in that rating. The graphic uses a red triangle icon labelled as "partial" for the CrowdStrike data, but does not explain what that means.

78. Unlike the free Security Value Map documents, the full paid report released on February 14, 2017 acknowledges at least some of the flaws in the CrowdStrike Falcon Platform ratings: [redacted] **Exhibit 9** at 2 (emphasis added). But even this purported disclaimer is false and misleading. In the draft report NSS provided the Court in response to CrowdStrike's request for temporary restraining order, NSS acknowledged that the final rating [redacted] Dkt. No. 8, Ex. 1 at 2 (emphasis added). But the consumers who only review and use the free Value Map documents do not receive any such notice.

79. The unqualified "Caution" rating in the Security Value Map document is also false and misleading because NSS' Test Methodology Advanced Endpoint Protection (AEP) v1.0 document ("AEP Methodology") states that a "Caution rating from NSS indicates that a product has performed poorly." But as above, NSS has acknowledged that [redacted] Dkt. No. 8, Ex 1 at 2.

80. On information and belief, the differences between the publicly available free Security Value Map documents and the paid report and draft report demonstrate that NSS' misrepresentations were willfully false and misleading.

81. NSS also falsely stated that the testing of the CrowdStrike Falcon Platform followed NSS' testing methodology. For example, on page 8, the Security Value Map documents' "Overall Ratings" do not follow the AEP Methodology, which states that *all* summary product guidance ratings will be based on five evaluation criteria. However, the ratings in the Security Value Map document and graphic for CrowdStrike were only based on two, not five as advertised. Again, NSS concealed this in the free version of the documents.

82. Additionally, on information and belief, NSS also did not follow the AEP Methodology in setting up and configuring the Falcon Platform for the comparative test. The AEP Methodology states that the "AEP product should be deployed in the 'default' prevention and/or protection mode ... based on common 'best practices' recommendations adopted by enterprises ... Product configuration, policies, and controls (access and application) that are implemented on the agent must mimic true enterprise endpoint deployments." But NSS' comparative test did not mimic a true enterprise deployment: CrowdStrike's review of the telemetry and audit logs shows that prevention settings were turned off during the entire test period, far from mimicking a true enterprise deployment. But even though no malware prevention can occur with the prevention settings disabled, NSS' report still claims that certain percentages of malware were prevented during testing, further demonstrating the flaws with NSS' testing and scores for the Falcon Platform. On information and belief, NSS knowingly misrepresented that the settings it used for CrowdStrike's Falcon Platform mimicked enterprise deployment. For example, NSS' private test agreement heavily emphasized [redacted]. Even if NSS did not use settings learned from CrowdStrike in its comparative test because those were CrowdStrike's Confidential Information, it knew that complete disabling of the prevention settings did not represent the default deployment mode of the Falcon Platform, the mode NSS advertises it used.

83. NSS' public statements about the way it accesses products for testing are also false and misleading. NSS states that "vendors do not get to choose whether or not they will be tested" and "if they decline... products for testing are typically purchased, but may also be donated by interested parties, and we will conduct the testing independently."[5] But neither of those scenarios

[5] https://www.nsslabs.com/security-test/nss-labs-test-policies/.

describes how NSS obtained Falcon access for its test after CrowdStrike declined to participate. NSS' attempt to purchase the tool was blocked. So, NSS engaged third parties to fraudulently obtain CrowdStrike credentials and secretly provide them to NSS, so it could fraudulently and illegally access CrowdStrike's Falcon Platform. Even had its license purchase been bona-fide, [redacted] had no right to provide access to NSS for testing and denies that it provided NSS access.

84. NSS also knowingly published a false and misleading numerical "security effectiveness score" for CrowdStrike in its free and paid reports. As noted, NSS' CEO Mr. Phatak admitted that NSS' inappropriate labelling of non-malicious programs as malware in private testing did not comply with NSS' own standards and made the testing flawed. NSS refused to delay the AEP comparative testing to fix those issues. On information and belief, the comparative test had similar flaws, and therefore NSS' security effectiveness score for CrowdStrike, obtained and calculated using tests that NSS knew and admitted were flawed, was false and misleading.

85. NSS' Security Value Map documents, and comparative reports, are also false and misleading where they directly compare the "security effectiveness" of different vendors' tools. Given that NSS' test of the Falcon Platform was admittedly incomplete, the reported scores for the Falcon Platform are based on a different number of samples and different sample set than the other vendors' tools. Any comparison between them is therefore misleading. Other vendors have also complained about NSS' undisclosed use of different sample sets for the different tools.[6]

86. Although CrowdStrike has stated its belief that NSS' testing results were incomplete and invalid, potential CrowdStrike customers are still confused, misled, and have sought more information from CrowdStrike about the tests. CrowdStrike personnel and resources

[6] *See, e.g.*, https://www.eset.com/us/about/newsroom/corporate-blog/eset-recounts-experience-with-nss-labs-and-aep-10-test/.

have been diverted to responding to customer questions about NSS' false and misleading publications, and some sales have been lost as a result. Moreover, the damage caused by NSS' false and misleading statements is exacerbated because, unlike reputable testing companies, NSS does not sufficiently disclose its testing methodologies, or its adherence to them in testing, thereby making it impossible for vendors to verify and/or refute results (particularly where vendors have not participated in a private test).[7]

V. CAUSES OF ACTION

COUNT I
(Violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030))

87. CrowdStrike hereby restates the averments contained in the foregoing paragraphs as if fully set forth herein.

88. The Falcon Platform is password protected and access requires CrowdStrike authorization. To use the Falcon Platform, a user must enter credentials provided by CrowdStrike to access computers hosted and operated by CrowdStrike, first to obtain and install the Falcon Agent locally, and then to access system feedback through the Falcon Dashboard. During operation, the Falcon Agent on a user device communicates with the Falcon Cloud, also hosted on computers operated by CrowdStrike.

89. Such CrowdStrike computers are used in and affect interstate commerce or communications.

90. CrowdStrike expressly prohibited NSS from accessing the Falcon Platform with any third party's credentials.

91. NSS knew it was not authorized to access the Falcon Platform with a third party's

[7] *See, e.g.*, https://www.eset.com/us/about/newsroom/corporate-blog/esets-position-on-nss-labs-advanced-endpoint-protection-10-test-1/.

credentials, but did so anyway.

92. Through NSS' orchestrated scheme, it aided and abetted the trafficking of confidential login credentials and it fraudulently accessed the CrowdStrike Falcon platform without authorization.

93. By means of its unauthorized access, NSS obtained information about the operation of the Falcon Platform.

94. NSS's unauthorized access damaged CrowdStrike, including but not limited to impacting the integrity of data available in the customer's instance of the Falcon Platform and diverting and unnecessarily expending system resources.

95. In response to NSS' unauthorized access, CrowdStrike conducted an investigation to determine the circumstances of the unauthorized access, the damage such access caused, and how to respond to halt the unauthorized access and mitigate the damage. This investigation and remediation utilized significant company resources, including the time and attention of senior executives and employees, resulting in losses well in excess of $5,000.

96. As a direct and proximate result of NSS' unauthorized access, CrowdStrike has been damaged, and is likely to continue to be damaged, and NSS has been unjustly enriched. CrowdStrike is entitled to compensatory damages and disgorgement of any and all profits NSS made as a result of its wrongful conduct, in amounts to be proven at trial, an injunction prohibiting NSS from accessing the Falcon Platform without CrowdStrike's explicit authorization, and other equitable relief.

97. NSS' actions have caused and will continue to cause CrowdStrike irreparable harm if not preliminarily and permanently enjoined.

98. CrowdStrike has no adequate remedy at law.

COUNT II
(Copyright Infringement (17 U.S.C. § 501 et seq.))

99. CrowdStrike hereby restates the averments contained in the foregoing paragraphs as if fully set forth herein.

100. At all relevant times, CrowdStrike has been the producer and owner of the Falcon Platform, including the Falcon Agent software code.

101. CrowdStrike holds a copyright registration certificate from the United States Copyright Office for the Falcon Agent software code.

102. By its conduct alleged herein, NSS infringed the copyright in the Falcon Agent software code, including by downloading and thereby copying the Falcon Agent software onto NSS computers, and using that software.

103. NSS knew that the infringed work belonged to CrowdStrike and that NSS did not have permission to copy the work. NSS' acts of infringement were willful and in disregard of and with indifference to CrowdStrike's rights.

104. On information and belief, NSS profited from its willful infringement by using the CrowdStrike Falcon Platform to develop, market and sell its testing reports and its CAWS product.

105. As a direct and proximate result of NSS' infringement, CrowdStrike has been damaged, and is likely to continue to be damaged, including by damage to its reputation, loss of goodwill, and loss of sales, and NSS has been unjustly enriched. CrowdStrike is entitled to compensatory damages and disgorgement of any and all profits NSS made as a result of its wrongful conduct, in amounts to be proven at trial, and other equitable relief.

106. NSS' actions have caused and will continue to cause CrowdStrike irreparable harm if not preliminarily and permanently enjoined.

107. CrowdStrike has no adequate remedy at law.

COUNT III
(Misappropriation of Trade Secrets (18 U.S.C. § 1832 et seq.))

108. CrowdStrike hereby restates the averments contained in the foregoing paragraphs as if fully set forth herein.

109. CrowdStrike's Falcon Platform is used in, and intended for use in, interstate commerce.

110. The Falcon Platform contains CrowdStrike's trade secrets, including those outlined above. CrowdStrike's trade secrets are not generally known, are subject to reasonable measures to keep them confidential, and give CrowdStrike an economic advantage over competitors.

111. NSS misappropriated CrowdStrike's trade secrets by knowingly stealing such information, taking it without authorization, and obtaining it by artifice or deception.

112. NSS also misappropriated CrowdStrike's trade secrets by, without authorization, knowingly taking, using, altering, transmitting, communicating, and conveying such information.

113. NSS also misappropriated CrowdStrike's trade secrets by knowingly possessing such information knowing it was stolen and obtained without authorization, and refusing to return it to CrowdStrike.

114. NSS engaged in the foregoing acts with the intent to convert CrowdStrike's trade secrets for NSS' own economic benefit and knowing such acts would injure CrowdStrike.

115. As a direct and proximate result of NSS's misappropriation, CrowdStrike has been damaged, and is likely to continue to be damaged, including by damage to its reputation, loss of goodwill, and loss of sales, and NSS has been unjustly enriched. CrowdStrike is entitled to compensatory damages and disgorgement of any and all profits NSS made as a result of its wrongful conduct, in amounts to be proven at trial, and other equitable relief.

116. NSS' misappropriation was knowing, willful, malicious, and undertaken by NSS for its own financial gain, and therefore CrowdStrike is entitled to exemplary damages and reasonable attorney's fees and costs.

117. NSS' actions have caused and will continue to cause CrowdStrike irreparable harm if not preliminarily and permanently enjoined.

118. CrowdStrike has no adequate remedy at law.

COUNT IV
(False Advertising under the Lanham Act (15 U.S.C. § 1125))

119. CrowdStrike hereby restates the averments contained in the foregoing paragraphs as if fully set forth herein.

120. NSS' statements, including those discussed above, are false and misleading.

121. NSS' statements, including those discussed above, constitute commercial advertising or promotion, in that they invite customers to purchase NSS' commercial products, including subscriptions, reports, marketing rights to NSS' public rankings and testing information, and NSS' CAWS product.

122. NSS has a financial interest in misrepresenting its test policies and methodology, and in misrepresenting that its unauthorized comparative testing of CrowdStrike's Falcon Platform adhered to those policies and methodology. NSS made and makes these false and misleading statements to realize an economic gain, by using the statements to market and sell NSS' own commercial products, not for the purpose of informing the public.

123. NSS has made and continues to make the false and misleading statements for the purpose of influencing consumers to buy NSS' commercial products.

124. NSS' false and misleading statements are sufficiently disseminated to the relevant purchasing public to constitute advertising or promotion within the cybersecurity industry, because

NSS makes the statements on its website through which it sells its commercial products, as well as in press releases, press interviews, and at trade events.

125. NSS' false and misleading statements actually deceived, or have tendency to deceive, a substantial portion of NSS' intended audience, because the statements were directed to and received by relevant consumers who were exposed to the claims through various channels.

126. NSS' false and misleading statements are material in that they are likely to influence purchasing decisions, because CrowdStrike's and NSS' existing and prospective customers are likely to believe NSS' false or misleading claims about its comparative tests, believe that NSS' comparative testing of CrowdStrike's Falcon Platform adhered to NSS's published policies and methodology, and believe that the Falcon Platform did not compare well to competing products based on that methodology, and such claims are likely to make a difference to such customers. CrowdStrike's competitors in the marketplace have used NSS' false statements to promote their own products over CrowdStrike's.

127. NSS' false and misleading statements are likely to have an impact on Falcon Platform sales, because NSS' claims are likely to cause CrowdStrike's prospective or existing customers to question the efficacy of CrowdStrike's Falcon Platform and to purchase one of the alternative products that NSS gives higher ratings instead of purchasing the Falcon Platform. NSS' false and misleading statements have been raised in the sales process and have required CrowdStrike to address them.

128. The advertised goods—NSS' subscriptions, reports, marketing rights, and CAWS product, and CrowdStrike's Falcon Platform—travel in interstate commerce.

129. As a direct and proximate result of NSS' false or misleading statements, CrowdStrike has been damaged, and is likely to continue to be damaged, including by damage to

its reputation, loss of goodwill, and loss of sales, and NSS has been unjustly enriched. CrowdStrike is entitled to compensatory damages and any and all profits NSS made by its wrongful conduct, in amounts to be proven at trial, and other equitable relief.

130. NSS' false and misleading statements were knowing, willful, and malicious, and made by NSS for its own financial gain, and therefore CrowdStrike is entitled to reasonable attorneys' fees and costs.

131. NSS' actions have caused and will continue to cause CrowdStrike irreparable harm if not preliminarily and permanently enjoined.

132. CrowdStrike has no adequate remedy at law.

COUNT V
(Breach of Contract)

133. CrowdStrike hereby restates the averments contained in the foregoing paragraphs as if fully set forth herein.

134. The Private Agreement between NSS and CrowdStrike, which incorporates NSS' Terms of Service, is a valid and enforceable contract.

135. CrowdStrike has fully performed or tendered all performance required under the Private Agreement.

136. On information and belief, NSS breached its obligations under the Private Agreement and Terms of Service by using information about the Falcon Platform that NSS obtained pursuant to the Private Agreement to develop, market, and sell NSS subscriptions, reports, marketing rights, and CAWS product.

137. NSS also breached its obligations under the Private Agreement by failing to return or verify in writing the destruction of the Falcon software.

138. NSS also breached the Private Agreement by failing to perform the Private

Agreement in a professional or workman like manner by conducting two tests that were admittedly flawed and unacceptable.

139. NSS has breached the implied covenant of good faith and fair dealing by acting to deprive CrowdStrike of the benefits of the confidentiality and other provisions in the Private Agreement.

140. As a direct and proximate result of NSS' breaches, CrowdStrike has been damaged, and is likely to continue to be damaged, including by damage to CrowdStrike's reputation, loss of goodwill, and loss of sales, and NSS has been unjustly enriched. CrowdStrike is entitled to compensatory damages and disgorgement of any and all profits NSS made by its wrongful conduct, in amounts to be proven at trial, and other equitable relief.

141. NSS' actions have caused and will continue to cause CrowdStrike irreparable harm if not preliminarily and permanently enjoined.

142. CrowdStrike is entitled to specific performance.

143. CrowdStrike has no adequate remedy at law.

COUNT VI
(Tortious Interference with Contract)

144. CrowdStrike hereby restates the averments contained in the foregoing paragraphs as if fully set forth herein.

145. CrowdStrike's Terms and Conditions expressly forbid the use of authorized credentials to access the Falcon Platform other than by the customer or its authorized subcontractors, and expressly prohibit use of the Falcon Platform by or on behalf of competitors, for competitive analysis, and by anyone other than the customer except for specified internal purposes of the customer.

146. Thomason, and/or [redacted] had to, and on information and belief, did click to

accept CrowdStrike's Terms and Conditions when they activated login credentials to the Falcon Platform, and before downloading the Falcon Agent software. In addition, [redacted] Quote and subsequent Purchase Order for the Falcon Platform, signed by Thomason [redacted].

147. NSS was provided with a copy of CrowdStrike's customer Terms and Conditions, and informed in writing about their provisions, prior to NSS' unauthorized access to the Falcon Platform for comparative testing.

148. NSS was aware that CrowdStrike's Terms and Conditions forbid all customers from providing Falcon Platform access (including Falcon Agent software, related trade secrets or confidential information) to third parties, and prohibit Falcon Platform access or use by competitors, for competitive analysis, and by anyone other than the customer except for specified internal purposes of the customer, because CrowdStrike told NSS about those prohibitions prior to NSS' unauthorized access to the Falcon Platform for comparative testing.

149. Nonetheless, NSS induced one or more third parties (*e.g.*, Thomason and/or [redacted] to obtain access to the Falcon Platform, and to provide NSS with access to the Falcon Platform, including Falcon Platform credentials and Falcon Agent software in violation of CrowdStrike's Terms and Conditions.

150. NSS obtained access to the Falcon Platform, including obtaining Falcon Platform credentials and a copy of the Falcon Agent software, from or through [redacted] and/or Thomason after being told by CrowdStrike that such acts would violate the customer's Terms and Conditions of service, thereby inducing a breach of the third parties' contractual obligations to CrowdStrike.

151. NSS repeatedly used the Falcon Agent software and repeatedly accessed the Falcon

Platform using credentials obtained from the third parties after being by CrowdStrike that such acts would violate the customer's Terms and Conditions of service, thereby inducing a breach of the third parties' contractual obligations to CrowdStrike.

152. In addition, NSS claims that the third parties knew that NSS would obtain access to the Falcon Platform and Falcon Agent software through their actions, demonstrating that NSS intentionally and willfully caused the third parties to violate their contractual obligations to CrowdStrike.

153. NSS has refused to return or destroy the copy of the Falcon Agent software obtained through the third parties, and any data obtained through its unauthorized access, even after receiving explicit instructions from both CrowdStrike and Thomason to do so.

154. NSS did not secure CrowdStrike's permission to use data obtained from the Falcon Platform in NSS' AEP comparative test or CAWS product.

155. On information and belief, NSS used data from the Falcon Platform that NSS obtained access to without authorization through Thomason and [redacted] to develop, market, and sell NSS subscriptions, reports, marketing rights, and CAWS product.

156. NSS had no justification for its actions.

157. As a direct and proximate result of NSS' tortious interference with CrowdStrike's contractual relationships, CrowdStrike has been damaged, and is likely to continue to be damaged, including by damage to its reputation, loss of goodwill, and loss of sales, and NSS has been unjustly enriched. CrowdStrike is entitled to compensatory damages and disgorgement of any and all profits NSS made by its wrongful conduct, in amounts to be proven at trial, and other equitable relief

158. NSS' actions have caused and will continue to cause CrowdStrike irreparable harm

if not preliminarily and permanently enjoined.

159. CrowdStrike has no adequate remedy at law.

COUNT VII
(Common Law Fraud)

160. CrowdStrike hereby restates the averments contained in the foregoing paragraphs as if fully set forth herein.

161. In early 2016, CrowdStrike entered into the Private Agreement with NSS, and provided NSS labs with limited access to its Falcon Platform, solely for the purpose of private testing. The Private Agreement made clear that [redacted]

162. Because NSS repeatedly failed to perform testing in a competent fashion, and twice provided results that were admittedly flawed and unacceptable, CrowdStrike never provided any such [redacted] to NSS. Rather, CrowdStrike expressly told NSS that it was not authorized to access the Falcon Platform for comparative testing.

163. Because CrowdStrike would not authorize comparative testing, in or before December 2016, NSS (on information and belief, through its CEO, Vikram Phatak and/or CTO, Jason Brvenik) engaged David Thomason to find a company willing to pose as a customer, enter into a Falcon Platform license with CrowdStrike, and then provide the access credentials to NSS. According to NSS, NSS agreed with Thomason and [redacted] that it would pay for the customer's license if it could obtain covert access to the Falcon Platform.

164. On or about January 5, 2016, pursuant to that side agreement with NSS and on NSS' behalf, Thomason submitted a fraudulent purchase order for the Falcon Platform, ostensibly on behalf of [redacted] According to NSS, both Thomason and [redacted] knew that the

license was being sought for NSS to gain access, and knew that NSS promised to pay for the license. Despite such knowledge, NSS and Thomason falsely identified [redacted] as the [redacted], concealing that NSS was real-party in interest seeking to gain access to CrowdStrike products through the purchase order. The purchase order was also knowingly fraudulent in suggesting Thomason was the [redacted], concealing that [redacted]. On information and belief, Thomason knowingly never intended to pay for the license because [redacted]. Yet, on information and belief, NSS never intended to pay, and in fact has never paid [redacted]. On information and belief, NSS and Thomason knew the purchase order was fraudulent when they submitted it.

165. On information and belief, the submission of the fraudulent purchase order to CrowdStrike was done at the direction of NSS and for its benefit. NSS and Thomason knew the purchase order contained the above false statements, and they intended CrowdStrike to rely on them, so that CrowdStrike would not reject the order and NSS could illicitly gain access to the Falcon Platform without CrowdStrike's knowledge.

166. CrowdStrike justifiably relied on the false representations in the purchase order when it approved the purchase order and provided login credentials to the Falcon Platform to Thomason. CrowdStrike was unaware that NSS would be gaining access and CrowdStrike had no way of knowing that the purchase was fraudulent and had been orchestrated by NSS to illicitly obtain the credentials, as that information was concealed from the purchase order and the credentials request. Had the purchase order identified NSS, CrowdStrike would not have approved it.

167. As a direct and proximate result of NSS' fraud, CrowdStrike was induced to enter

into a license with [redacted] for the Falcon Platform. CrowdStrike is entitled to rescission of the license agreement with [redacted]

168. As a further direct and proximate result of NSS' fraud, NSS gained access to, accessed and used CrowdStrike's Falcon Platform without authorization, and illicitly gathered confidential information about CrowdStrike's products that NSS used to prepare, market and sell reports and, on information and belief, used to build, market and sell its CAWS product. NSS used its fraudulent access to the CrowdStrike's Falcon Platform for its own financial gain, including unjustly profiting from its inclusion of information about CrowdStrike's Falcon Platform in NSS products. CrowdStrike has been damaged, and is likely to continue to be damaged, including by damage to its reputation, loss of goodwill, and loss of sales, and NSS has been unjustly enriched. CrowdStrike is entitled to compensatory damages and disgorgement of all profits NSS made by its wrongful conduct, in amounts to be proven at trial, and other equitable relief.

169. NSS' actions have caused and will continue to cause CrowdStrike irreparable harm if not preliminarily and permanently enjoined.

170. CrowdStrike has no adequate remedy at law.

171. NSS's fraud was willful and malicious.

WHEREFORE, CrowdStrike prays for the following relief:

a. For the entry of a judgment compelling NSS to specifically perform its obligations under the Private Agreement, to include returning or confirming in writing the destruction of all CrowdStrike software, credentials, passwords, etc.;

b. For entry of a preliminary injunction, and permanent injunction for the following relief, or such other relief as the court may order:

(i) ordering NSS to refrain from accessing or using any CrowdStrike Falcon Platform, trade secrets, or Confidential Information, for any purpose;

(ii) ordering NSS to refrain from publishing any false or misleading statements concerning NSS' policies or methodology regarding its comparative tests, its adherence to those policies or methodology, in its comparative test of CrowdStrike's Falcon Platform, the results of such test, or other information concerning CrowdStrike or its technology or products;

(iii) ordering NSS to comply with all contractual terms including destruction or return of the Falcon Agent software and any other CrowdStrike technology or confidential information;

(iv) ordering NSS to refrain from using any data obtained from the Falcon Platform in NSS' private or comparative tests, subscriptions, reports, marketing rights, or CAWS product; and,

(v) ordering NSS to identify all circumstances in which NSS has provided CrowdStrike technology or information to third parties, and to ensure the return or destruction of all such technology and information;

c. For such further relief as may be appropriate, including but not limited to:

(i) monetary damages;

(ii) exemplary damages;

(iii) disgorgement of NSS profits;

(iv) an accounting and constructive trust;

(v) pre-judgment and post-judgment interest; and,

(vi) reasonable attorneys' fees and costs.

Plaintiff demands a jury trial on all issues triable by jury.

POTTER ANDERSON & CORROON, LLP

/s/ David Ellis Moore

David E. Moore (#3983)
Bindu A. Palapura (#5370)
Stephanie E. O'Byrne (#4446)
1313 N. Market St., Hercules Plaza, 6th Floor
P.O. Box 951
Wilmington, DE 19899-0951

Of Counsel:

Ryan Tyz

Erin Jones
Aaron Myers
TYZ LAW GROUP PC
4 Embarcadero Center, Suite 1400
San Francisco, CA 94111
(415) 849-3578
rtyz@tyzlaw.com
ejones@tyzlaw.com
amyers@tyzlaw.com

(302) 984-6000
dmoore@potteranderson.com
sobyrne@potteranderson.com
bpalapura@potteranderson.com

Attorneys for Plaintiff

Dated: January 10, 2018
Public Version Dated: January 18, 2018